[19]中华人民共和国专利局

[51]Int.Cl[6]
H04L 9/00

[12] 发明专利申请公开说明书

[21] 申请号 96121033.8

[43]公开日 1997 年 9 月 10 日

[11] 公开号 CN 1159112A

[22]申请日 96.10.16

[30]优先权

[32]95.10.16[33]JP[31]267250 / 95

[71]申请人 索尼公司

地址 日本东京都

[72]发明人 石黑隆二

[74]专利代理机构 柳沈知识产权律师事务所

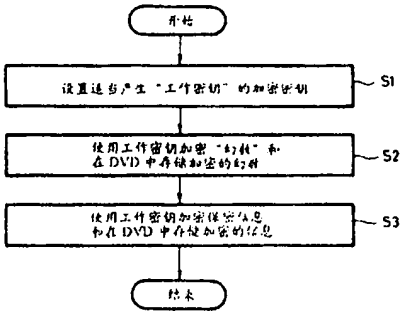
代理人 孙履平

权利要求书 3 页 说明书 12 页 附图页数 9 页

[54]发明名称 加密方法及装置、记录方法、解码方法及装置和记录介质

[57]摘要

本发明提供了加密方法；加密装置；记录方法；记录装置解码方法；解码装置和记录介质，其中加密密钥能够容易地使用分级的加密密钥加以管理。



权　利　要　求　书

1、一种使用预定的加密密钥加密预定信息的方法，包括下述步骤：

使用单向函数对所说的加密密钥进行分级；和

使用所说分级的加密密钥对所说的预定信息进行解码。

2、如权利要求1的方法，其中，经分级的加密密钥的第一级加密密钥是主密钥。

3、如权利要求1的方法，其中，使用所说分级的加密密钥加密特定的信息。

4、一种将预定的加密信息记录到记录介质上的方法，包括以下步骤：

接收通过使用单向函数分级加密密钥加密的预定的信息；和

将所说加密的预定信息记录到所说的记录介质上。

5、如权利要求4的方法，其中，进一步包括接收通过使用所说加密密钥加密的特定信息和将所说加密的预定信息与所说加密的特定信息一块记录到所说的记录介质上的步骤。

6、一种解码加密预定信息的方法，包括步骤：

接收加密的预定信息；和

通过使用解码密钥对所说加密的预定信息进行解码解码密钥对应单向函数分级的加密密钥。

7、如权利要求6的方法，其中，所说分级加密密钥的第一级加密密钥是主密钥和对应于加密密钥的解码密钥是通过使用所说单向函数从所说主密钥中产生的。

8、如权利要求6的方法，其中，进一步包括接收加密特定信息，确定对应于加密密钥的解码密钥的步骤，该加密密钥对接收来自特定信息中的加密预定信息、加密特定信息、和确定对应加密密钥的解码密钥所使用信息进行加密和使用确定的解码密钥对加密的预定信息进行解码。

9、如权利要求8的方法，其中，用于确定对应于所说加密密钥的所说解码密钥的信息是主密钥信息或最后一个加密密钥的信息。

10、如权利要求8的方法，其中，所说确定对应于所说加密密钥的解码密钥的步骤包括。

(a)将确定对应于加密密钥的解码密钥的信息用来解码所说加密的预定

的信息；和

比较解码的特定信息和所说特定信息以及根据比较的结果确定对应于加密密钥的解码密钥。

11、如权利要求 10 的方法，其中，如果确定，所说解码的特定信息和所说特定信息相互一致，那么用于确定对应于加密密钥的解码密钥的当前信息就是解码加密预定信息的解码密钥，和如果确定，所说 解码的特定信息和所说特定信息不相一致，那么用于确定对应于加密密钥的解码密钥的当前信息是被单向函数分级的和对应于加密密钥的解码密钥由重复所说步(a)和(b)的步骤加以确定。

12、如权利要求 6 的方法，其中，将所说加密的预定信息记录在记录介质上，所说加密的预定信息从所说的记录介质读出并提供，和所说的加密密钥以对应所说加密密钥的字符、数字、条形码或全息图的形式复制在所说的记录介质或存储在所说记录介质上。

13、如权利要求 6 的方法，其中，将所说加密密钥插入到用于解码加密的预定信息的预定的软件作为对应于所说加密密钥的代码。

14、如权利要求 6 的方法，其中，所说加密密钥通过电话线网络或网络加以提供。

15、一种使用预定加密密钥对预定信息进行解码的装置，包括:

产生加密密钥的装置，用于通过使用单向函数分级 加密密钥产生加密密钥；和

解码装置，用于使用所说分级的加密密钥解码所说预定信息.

16、如权利要求 15 的装置，其中，所说分级加密密钥的第一级密钥是主密钥。

17、如权利要求 15 的装置，其中，进而包括使用所说分级的加密密钥对特定信息进行加密的装置。

18、一种解码加密的预定信息的装置，包括:

接收装置，用于接收所说加密的预定信息；和

解码装置，用于使用对应于由单向函数分级的加密密钥的解码密钥解码所说加密的预定信息。

19、如权利要求 18 的装置，其中，进而包括第一存储器，存储用来确定对应于所说加密密钥的解码密钥的信息；产生装置使用单向函数从所说的

主密钥产生对应于加密密钥的解码密钥和第二存储器存储对应于产生的加密密钥的解码密钥　和其中用于确定对应于所说加密密钥的解码密钥的信息是所说分级密钥的第一级加密密钥即主密钥.

20、如权利要求 18 的装置，其中，进而包括接收装置，用于接收加密的特定信息和其中，所说的产生装置确定对应于加密密钥的解码密钥，它加密从特定信息中所接收的加密的预定信息、加密的特定信息和确定对应于加密密钥的解码密钥的信息和所说的解码装置使用确定的解码密钥解码所说加密的预定的信息.

21、如权利要求 20 的装置，其中，所说确定对应于加密密钥的解码密钥的信息是主密钥的信息或是最后一个加密密钥的信息.

22、如权利要求 21 的装置，其中，所说的产生装置由用来确定对应于加密密钥的解码密钥的所说信息对所说加密的预定的信息进行解码，比较解码的特定信息和所说的特定信息和根据比较的结果确定对应于加密密钥的解码密钥.

23、如权利要求 22 的装置，其中，如果确定，所说解码的特定信息和所说特定信息相互一致，那么，所说产生装置确定，用来确定对应于加密密钥的解码密钥的当前信息是解码加密预定信息的解码密钥和存储所说解码密钥到所说的第二存储器和如果确定，所说解码的特定信息和所说特定信息并不相互一致，那么所说产生装置使用单向函数对确定对应于所说加密密钥的解码密钥的当前信息进行分级和通过重复权利要求 22 的操作确定对应于加密密钥的解码密钥.

24、如权利要求 19 的装置，其中，所说第一存储器，所说第二存储器，所说的产生装置和所说的解码装置均放置在单个的 IC 芯片内.

25、如权利要求 24 的装置，其中，所说的用来确定对应于所说加密密钥的解码密钥的信息事先存储在所说的第一存储器内.

26、一种使用解码装置可解码的记录介质，其中，所说的记录介质包括可被所说解码装置解码的记录信号和所说的记录信号包括使用单向函数分级的加密密钥加密的预定信息.

27、如权利要求 26 的记录介质，其中，所说的记录信号进一步包括使用所说加密密钥加密的特定信息.

28、如权利要求 26 的方法，其中，所说的加密密钥以对应于所说加密密钥的字符、数字、条码或全息图的形式复制在所说的记录介质上.

说　明　书

加密方法及装置、记录方法、解码方法及装置和记录介质

本发明涉及加密软件或数据的方法；加密软件或数据的装置；记录加密的软件或数据的方法；解码加密的软件或数据的方法；解码加密软件或数据的装置和用一种记录方法记录信息的记录介质，具体地，本发明涉及加密软件或数据的方法；；记录加密软件或数据的方法；解码加密软件或数据的方法；解码加密软件或数据的装置和为防止非法使用记录在记录介质上的软件或数据而提供使用的记录介质，例如为防止非法使用记录在数字视盘或通过网络提供的软件或数据而提供使用的记录介质。

为防止非法使用软件或数据，习惯上采用预定的加密密钥来加密软件和数据以及在数字视盘(以后简称为DVD)上记录加密软件和数据或由一网络传送加密的软件或数据，由此产生加密的软件或数据．记录在 DVD 上的加密软件或数据和由网络提供的加密软件和数据则由分别形成的加密密钥加以解码。

信息被加密和解码的方法将在下面简要地加以描述。

图 1 示出信息或数据被加密或解码的原理

发射机(101)使用加密密钥 K1 对明码文 M(要传送的信息)进行加密以提供加密电文 C(实际上要传送的数据)，该加密电文 C 被传送到接收机而该接收机(102)使用解码密钥 K2 对加密电文 C 进行解码以提供明码文 M，以这种方式，明码文从发射机传送到接收机，经常观察到，那些没有解码密钥(即，密码破译器(code_breakers))的人们用窃听器监听加密电文 C 和解码(103)加密电文 C，而那些有解码密钥的人们从加密电文 C 产生明码文 M 的方法，一般称为“解码”，而那些没有解码密钥的人们用窃听器监听加密电文 C 和从加密电文 C 得到明码文 M 的方法被称为“解密”。

然而，当明码文被以上述的加密密钥加密时，一旦加密密钥被解码，这样的加密密钥对防止非法使用就变得无效，因此，当加密密钥被解密时，就将该加密密钥更新为一个新的加密密钥，而软件或数据通过使用这样更新的加密密钥被加密，这样来防止非法使用软件或数据。

然而，在实践中，甚至当把加密密钥更新了时，也经常观察到，还存在着被先前加密密钥加密过的软件或数据，因此为解码这样的数据，先前的密钥就不得不被保留下来，其结果，每更新一次加密密钥，都要使保留的加密密钥增加，于是硬件和软件两者均面临着管理保留密钥的问题。

当用先前硬件的观点装配加密密钥时，为将这样的加密密钥更新成新的加密密钥，有时会非常困难。

有鉴于此，为解决现有技术中的上述问题的本发明的目的是提供一种加密方法；加密装置；记录方法；解码方法；解码装置和记录介质，其中加密密钥能够容易地由分级(hierarchizaing)加密密钥管理。

根据本发明的一个方面，提供了使用预定的加密密钥对预定的信息进行加密的方法。

该方法包括使用单向函数分级加密密钥和使用分级的加密密钥对预定的信息进行解码的步骤。

依照本发明的第二个方面，提供了在记录介质上记录预定加密信息的方法，该方法包括接收使用单向函数分级的加密密钥加密的预定信息和在记录介质上记录加密的预定信息的步骤。

依照本发明的第三个方面，提供了解码加密的预定信息的方法，该方法包括接收加密的预定信息和使用单向函数分级的加密密钥所对应的解码密钥解码加密的预定信息的步骤。

依照本发明的第四个方面，提供了使用预定的加密密钥解码预定的信息的装置，该装置包括使用单向函数分级加密密钥产生加密密钥的装置和使用分级的加密密钥对预定的信息进行解码的装置。

依照本发明的第五个方面，提供了解码加密的预定信息的装置，该装置包括接收加密的预定信息的装置和使用单向函数分级的加密密钥所对应的解码密钥对加密的预定信息进行解码的装置。

依照本发明的第六个方面，提供了能被解码装置解码的记录介质。该记录介质包括能由解码装置解码的记录信号和该记录介质包含着通过使用单向函数分级的加密密钥加密的预定信息。

本发明的目的、特征及优点将结合实施例参考附图进行详细描述

图 1 的示意图示出对软件或数据进行加密和对加密的软件或数据进行解码的原理；

图2的示意图示出可应用于加密方法的本发明的加密密钥分级结构一实例;

图3示出了将加密信息记录在DVD上的方法的流程图;

图4示出在其上面记录了加密幻数(magic)密钥和加密信息的DVD的示意图;

图5是本发明的加密装置的实例方框图;

图6是用于解码图4中示出的记录在DVD上信息的IC芯片11的实例方框图;

图7是用于解释图6中示出的IC芯片11的操作的流程图;

图8是用于解释图7示出的步骤S12的细节的流程图;

图9是用于解释图7示出的步骤12的细节的流程图;

图10的示意图是用来解释将加密密钥复制在DVD上和将其分配的方法;

图11的示意图是用来解释将加密密钥插入到解码软件和将其分配的方法;

图12的示意图是用来解释将加密密钥包括到集成电路中和将其分配的方法。

下面将参照附图描述本发明

图2是应用了本发明的加密方法的分级加密密钥的示意图.

如图2所示，通过使用所谓的单向函数F，相对于第一级的加密密钥(主密钥)K0形成下一级(Ver.n)的加密密钥K1．该单向函数F是所谓许多单向函数中的一种且它完成一种不可逆的计算，其中加密密钥K1能容易地从K0计算出来，但是逆计算却实际上不能进行，即，加密密钥K0实际上不能从K1中计算出来.

另一方面，作为单向函数，这里可以使用加密算法例如数据加密标准(DES, National Bureau of Standards FIPS Publication 46, 1977)，快速加密算法(FEAL, S.Miyaguchi.The FEAL Cipher family.Lecture Notes in Computer Science, 537(1001), pp 627 to 638 (Advances in Cryptology - crypto'90))或信息整理算法例如信息整理算法(MD4, R.L.Rivest.537(1001), PP303 to 311.(Advances in Cryptology - Crypto'90))或保密散列标准(SHS, Secure Hash Standard, National Bureau of Standards FIPS Publication 180, 1993)“由Tsujii和Kasahara在1993，

7 著的密码和信息保密” 中详细地描述了 DES 和 FEAL .

随后，单向函数将参照实施例详细地描述.

在 DES 情况下，单向函数和 DES 之间已经建立起一种关系并由下述式(1)表示:

$$F(K) = DES(IV. K) \quad (1)$$

这里 IV 是初始矢量并且是任意的， k 是密钥

然而，作为在单向函数中使用的算法，这里可以使用下述的表达式.

根据块(block)密码(乘积密码)算法；和算术算法

使用如下等式 (2)表示的密钥基本块密码(乘积密码)算法能通过对明码文加密获得密码电文:

$$C = Enc(P, K) \quad (2)$$

这里 C 是密码电文， P 是明码文，和 K 是密钥，

特别是，通过每块的特定类散列函数在该密钥上采用有效的不可逆变换能获得固定长度的位串.

然后，明码文被替代数据或类似几个循环(round)的置换箱或替换箱加以处理，在每一次循环(round)中，明码文都用从密钥，例如从“异”(exclusive-OR)逻辑计算中获得的位串通过特定计算加以处理.

算述算法在离散算法问题中被使用并由下述等式(3)加以表示:

$$F(K) <= => ak \bmod p \quad (3)$$

这里 a 是预定的常数， K 是密钥和 P 是素(Prime)数.

在上述的等式(3)中，符号<= =>表示 “定义”.

特别是，将函数 F(K)定义为 “对 K 乘 P 的乘积进行除法运算得到的余数” 在这种情况下函数 F(K)能够从密钥(K)容易地获得，但是从函数 F(K)获得密钥(K)是非常困难的.

如上所述，通过使用单向函数(F)从主密钥获得加密密钥 K1 之后，使用由下述等式(4)所表示的单向函数(F)可以顺序地计算加密密钥 K2， K3，...，Kn - 1， Kn，由此产生形成的分级加密密钥(Ver.n 至 Ver.1)

$$K_i = F(K_{i-1}) \quad (4)$$

这里 i = 1， 2， 3， ...， n

数字值 n 是分级的足够数目(级的数).

如上所述，虽然新的加密密钥能够容易地使用单向函数(F)加以计算，但

实际上逆计算不能被进行，即，原有的密钥(original key)实际上不能使用单向函数(F)从诸加密密钥中加以计算。

依照本发明加密信息例如加密软件或数据和将加密信息提供给用户的方法将在下面加以描述。如图 2 所示，当信息例如软件或数据被加密和被提供给用户时，信息最初是使用加密密钥 Kn(Ver.l)加密的和该加密密钥 kn 以附在加密信息后面或以单独提供的方式分配给用户，用户可以使用加密密钥 Kn 解码该加密的信息。

当加密密钥 Kn 被解密时，信息例如软件或数据便由高一级的加密密钥 K_{n-1}(Ver.2)进行加密和将该加密密钥 K_{n-1} 分配给用户．类似地，每次当加密密钥被解密，信息便由高一级的加密密钥进行加密和将该加密密钥分配给用户。

最初分配的最低一级的加密密钥 Kn 是通过函数(F)由下一级的加密密钥 K_{n-1} 计算出来的。特别是，加密密钥 Kn 可通过函数(F)容易地计算出来和使用加密密钥 Kn 加密的信息能使用由加密密钥 K_{n-1} 计算出来的加密密钥 Kn 加以解码。因此，由于该加密密钥是通过使用函数(F)由下一级的加密密钥计算出来的，下一级的加密密钥能通过使用函数(F)在任何级(generation)的情况下加以计算。因此，如果用户保留不能被解密的最终的加密密钥，那么用户不仅能对最终加密密钥加密的信息进行解码，而且能对先前加密密钥加密的信息进行解码，进而，所有加密密钥均是使用单向函数(F)由主密钥顺序产生的。因此，如果用户保留主密钥而不是保留还没有被解密的最后一个加密密钥，那么用户可以使用所有的加密密钥去解码加密的信息。这样，加密密钥可以容易地被管理。

图 3 的流程图使用以图 2 所示的诸加密密钥为例来解释将信息(明码文)例如将移动的图象、声音、数据或软件加密和将其记录在例如数字视盘(例如 DVD 和以后称为“ DVD ”)记录介质上的方法。

参看图 3，随着操作的开始，适当级的加密密钥(分级)在步骤 S1 中从图 2 所示分级的加密密钥中选出和将选出的加密密钥设置为工作密钥。然后，控制进入步骤 S2 ，这里，将一预定数目的字符串和字符设置为幻数(magic number)，使用在步骤 S1 获得的工作密钥对幻数进行加密，通过加密获得的加密幻数被记录在图 4 示出的 DVD1 的预定部分，作为一例。

此后，控制进入到步骤 S4 ，在此加密的数据，即通过使用工作密钥进

行加密的明码文和加密的数据(密码电文)被记录在图 4 示出的 DVD1 的预定的部分.

参照图 5 将描述上述加密方法的加密装置.

如图 5 所示，将明码文数据和幻数分别提供到端点 60， 70．将从端点 60、 70 来的明码文数据和幻数分别提供给相应的加密电路 51， 52．如上所述，幻数是预定数目的字符串和字符．工作密钥产生电路 53 从图 2 示出的分级的加密密钥中选出适当级(generation)的加密密钥和向加密电路 51， 52 提供该选出的加密密钥作为工作密钥．该加密电路 52 使用从工作密钥产生电路提供到此的工作密钥对提供的幻数进行加密．这样由加密获得的加密幻数提供给记录装置 54．加密电路 51 使用工作密钥对提供的明码文数据进行加密和提供加密的信息到记录装置 54．如图 4 所示，记录装置 54 将加密信息和加密幻数信息记录到 DVD1 的预定部分．

如果记录装置 54 是产生主盘的成型器，那么模子(stamper)从主盘形成和大量的盘可以使用这样的模子产生．

图 6 方框图示出 IC 芯片(chip)，为了重放这样制成的 DVD1，解码在光盘播放机(DVD 播放机，以后称为“ DVD 播放机”)内 DVD1 上记录的加密信息．幻数加密幻数和加密的信息(密码电文)均输入到 IC 芯片 11．加密的幻数从 DVD1 中提供，幻数是存储在 DVD 播放机本身的存储器内(未示出)和由这样的存储器提供．该幻数是预定数目的信息串和字符．该幻数与在加密侧使用的幻数相同．

存储器 12 存储图 2 示出的加密密钥 K0，即主密钥．寄存器 13 存储由使用相对于主密钥即工作密钥的函数(F)而获得预定级(generation)的加密密钥，这将在以后继续阐明．解码电路 14 根据输入的幻数；加密的幻数和从存储器 12 读出主密钥产生工作密钥和提供该形成的工作密钥到寄存器 13，这将在以后阐述．解码电路 14 使用工作密钥对输入的和加密的信息(密码电文)解码和输出解码的数据作为明码文数据(明码文)．

在 DVD1 记录 IC 芯片 11 内的加密数据的方法将参照图 7 流程图加以描述．

参看图 7，随着操作的开始，在步骤 S11，加密的幻数从 DVD1 的预定的位置读出．然后，控制进入到 S12，在此工作密钥从步骤 S1 读出的加密幻数和从 DVD 播放机本身的存储器(未示出)读出的幻数中获得，这将在后结

合图 8 流程图描述.

图 8 的流程图用来更详细地解释图 7 步骤 S12 的过程.

参看图 8，随着步骤的开始，最初，在步骤 S21，主密钥从 IC 芯片 11 的存储器中读出和设置为选择密钥(K). 然后，将该选择密钥(K)提供给解码电路 14．该选择密钥(K)表示当前被选取的加密密钥.

如图 8 所示，控制进入下一确定步骤 S22，在此将幻数和加密的幻数(magic)均提供给解码电路 14 和在此对加密的幻数使用选择密钥(K)解码. 然后，在确定步骤 S22 中确定使用选择密钥(K)对加密的幻数进行解码的结果是否与该幻数一致. 如果解码的结果和还未解码的幻数相互不一致，那么在确定步骤 S22 表示为 NO，即确定，该选择密钥不是在加密侧对加密的幻数进行加密的加密密钥. 接着控制回到步骤 S23，在此下一级的加密密钥通过使用由下述方程(5)表示的单向函数从选择密钥(K)中加以计算和设置一新的选择密钥(K):

$$K = F(K) \qquad (5)$$

然后，控制返回到步骤 S22，重复地执行类似地处理.

另一方面如果使用选择密钥(K)对加密幻数进行解码的结果和没被解码的幻数相互一致并在确定步骤 S22 表示为 YES，那么就确定该选择密钥(K)是对加密的幻数进行加密的加密密钥. 这样控制便进入到步骤 S24，其中解码电路 14 选取该选择密钥(K)作为工作密钥和将该选择密钥(K)提供到寄存它的寄存器 13．然后，图 8 流程图的处理结束和控制返回到图 7 流程的处理.

此后，控制进入图 7 流程的步骤 S13，在此解码电路 14 从寄存器 13 中读出在步骤 S12(图 8 中的步骤 S21 至 S24)中获得的工作密钥和使用工作密钥对输入到解码电路 14 中的加密信息(密码电文)进行解码和输出解码信息作为明码文数据(明码文).

如上所述，由于 IC 芯片获得了对应于来自主密钥的加密信息的工作密钥和使用该工作密钥解码输入的加密信息，如果用户仅保留了该主密钥，那么该用户能解码由任何级(generation)的加密密钥所加密的信息.

当上述的处理是由计算机软件完成时，图 7 步骤 S12 的处理可以由图 9 示出的流程图代替. 图 9 的流程图示出了在由软件实现图 6 示出的功能的计算机内解码加密信息的方法. 在这种情况下，计算机装入对应图 6 的解码电路板和该软件存储在该解码电路板的存储器内. 然而，在这种情况下，事先

存储在存储器内的主密钥并不使用，而使用最后分配的一个加密密钥(或可能是主密钥)被使用。

参照图 10 将描述，例如用户通过键盘以复制 DVD 的形式将配给的预定级的加密密钥(Ki)(这里 i 表示 n， n－1，...， 1 中的任何一个)输入计算机。将这样的加密密钥存储在计算机内的预定存储器。另外，计算机通过电话网络线或网络收到最后分配的加密密钥和在预定的存储器内(例如 RAM(随机存取存储器)) 存储。

参看图 9，随着操作的开始，在第一步骤 S31，将输入的预定级加密密钥(Ki)从存储器中读出和设置为选择密钥(K)。该选择密钥表示为当前选取的加密密钥，这类似于前述。

然后控制进入到确定步骤 S32，在此从存储器读出的幻数和从 DVD 上读出的加密的幻数均被提供和将加密的幻数由选择密钥(K)解码。在确定步骤 S32，它确定由选择密钥(K)解码加密的幻数的结果是否和幻数相一致。如果解码结果和没有加密的幻数相互不一致并且在确定步 S32 表示为 NO，那么，它可以确定选择密钥(K)不是加密该加密的幻数的加密密钥。这样，控制进入到步骤 S33，在此使用单向函数(F)从选择密钥(K)计算下一级(generation)的加密密钥和将这样计算的下一个级(generation)的加密密钥设置为新的选择密钥(K)。

然后，控制返回到步骤 S32 和重复地执行类似的处理。

另一方面，如果使用选择密钥解码加密的幻数的结果和幻数相互一致并且在确定步骤 S32 表示为 YES，那么，就可以确定该选择密钥是加密该加密幻数的加密密钥。这样，控制进入到下一步 S34，将该选择密钥(K)设置为工作密钥和将该工作密钥存储在预定的存储器内(即寄存器内)。这样，图 9 的 流程图的处理结束和控制返回到图 7 的流程图。

此后，控制进入到图 7 流程图步骤 S13，在此对加密的信息使用由步骤 S12(在图 9 的步骤 S31 至 S34)获得的工作密钥进行解码并输出明码文数据(明码文)。

如上所述，当由计算机软件加密的信息被解码时，根据分配的任意级的加密密钥，这就有可能使用加密密钥(Ki)或比加密密钥(Ki)级低的诸加密密钥(K_{i-1}至 K1)对加密的信息进行解码。

如上所述，依照本发明的实施例，由于用先前的加密密钥加密的信息能

根据最后的加密密钥(可以是主密钥或任意级的加密密钥)被解码，仅需将最后一级的加密密钥存储就足够了．因此，不同先有技术，每当加密密钥被解密和加密密钥被变化时，除了先前的加密密钥以外，新的加密密钥均不需要存储．这样，加密密钥能容易地被管理．

进而，在图 6 所示的实施例中，由于加密密钥(主密钥)是存储在 IC 芯片 11 内设置的存储器 12 内，预定级的加密密钥在 IC 芯片 11 内被计算和加密的信息被解码，加密密钥可以被防止泄露到外面和对加密密钥的解密是困难的．进而，在上述的实施例中，由于计算工作密钥的过程和解码加密信息的过程能使用同一个解码电路 14 完成，该电路能被节省．

分配加密密钥的方式将参照图 10 至 12 加以描述．

图 10 示出了将加密密钥复制在 DVD 的装置上或 DVD 本身上和被分配的方法．

如图 10 所示，对应于预定级的加密密钥的字母数字字符、条码、全息图或类似物被复制在 DVD21 的装置(case)上并且标题 A 也记录在上面或在 DVD21 本身的表面上．类似地，对应于预定级的加密密钥 B 的字母数字字符、条码、全息图或类似物复制在 DVD22 的装置(case)上和标题 B 也记录在其上面或在 DVD22 本身表面上，以这样的方式加密密钥 A 随同 DVD21 能够分配给用户和加密密钥 B 随同 DVD22 能够分配给用户．

另外，指示加密密钥 A 的数据可以记录在例如 IC 卡的记录介质上然后和 DVD21 一块分配给用户或指示加密密钥 B 的数据可以记录在例如 IC 卡的记录介质上然后和 DVD22 一起分配给用户．

当用户重放 DVD21 时，用户使用例如键盘的输入装置把复制在 DVD21 上的加密密钥 A 输入计算机 23．参考对图 9 流程图的 叙述，计算机 23 执行图 6 所示 IC 芯片 11 的功能，即依照预定的应用程序对加密信息进行解码的功能．

然后，当 DVD21 被设置到 DVD 读出器时(未示出)，计算机 23 通过 DVD 读出器从 DVD21 中读出加密信息和根据先前输入的加密密钥 A 对从 DVD21 中读出的加密信息进行解码。当然，记录在 DVD22 上的加密信息也可以以 DVD21 同样的方式进行解码．

依此，该情况适合于在每一个 DVD 标题上分配不同的加密密钥．例如，可以将使用单向函数从不同的主密钥计算出的诸加密密钥分配给 DVD 的每

个标题.

进而，甚至当对应于标题 A 的加密密钥 A 被解密时，将对应于标题 A 的加密密钥 A 更新为高一级的加密密钥 A2 和标题 A 的连续信息被加密密钥 A2 解码，还没有更新的加密密钥 A 通过使用参照图 9 流程图和类似上述的预定计算可以容易地获得. 因此，用户使用先前加密密钥及仅使用最后的加密密钥(在这种情况下，加密密钥 A2)就能对加密的标题 A 进行解码.

图 11 是将 加密密钥的代码指示插入到解码加密密钥的软件和分配给用户的方法.

如图 11 所示，将加密密钥的代码指示插入到解码加密信息的解码板所配置的解码软件上. 然后，该解码板 33 被装入计算机 23 . 这样计算机 23 通过解码电路板 33 能够对记录在 DVD31 、 32 上的加密信息进行解码和输出对应解码信息的移动图象，静止图象和声音.

该例适合于将相同的加密密钥分配给用户的情况.

在该例的情况下，计算机 23 可以连接到电话网络线或网络上，通过电话网络线和网络更新的加密密钥可以分配给计算机 23 . 计算机 23 在解码该解码电路板 33 的软件内存储通过电话网络线或网络分配给它的最后一个加密密钥.

这样，计算机 23 能使用该加密密钥参考图 7 和 9 以类似于上述描述对记录在 DVD31 、 32 上记录的信息进行解码.

进而，被加密密钥加密的信息能通过电话网络线或网络提供给计算机 23 . 在这种情况下，计算机 23 能通过电话网络线或网络使用先前分配给的加密密钥对该信息进行解码.

参看上述对图 2 的描述，所有各级的诸加密密钥能通过使用单向函数(F)从分级的第一加密密钥(K0)中形成和该加密密钥 K0 能被用作为主密钥. 因此，如果将作为主密钥的加密密钥插入到例如集成电路(IC)的硬件中，那么所有各级的诸加密密钥均能从该加密密钥 K0 形成和能解码由诸加密密钥(K1 至 Kn)的任一个加密的信息. 因为由用户解密插入到例如集成电路的硬件中的数据是非常困难的，故非法使用加密密钥能被抑制.

图 12 示出了将加密密钥插入到集成电路和被分配的方法. 如图 12 所示，有法律义务保密的制造者制造的主密钥被存储在集成电路 41 中， IC 芯片 11 能被应用到集成电路 41 . 在该例的情况下该集成电路 41 被提供给制造

者 A，然后，在将集成电路 41 装入 DVD 播放机 43 之后，该集成电路 41 被分配给了用户。

另一方面，将使用存储在集成电路 41 内的预定级的加密密钥加密的幻数和由该加密密钥加密的预定信息记录在 DVD42 上。

当用户把 DVD42 放在 DVD 播放机 43 时，主密钥从集成电路 41 中读出和工作密钥以参考图 7 和 8 流程图描述的方式相同的方式获得，依此将记录在 DVD42 上的加密信息解码和将对应的移动图象，静止图象和声音输出。

如上所述，当主密钥存储在集成电路中时，DVD 播放机 43 能够解码和输出记录在 DVD42 上的信息而不管对记录在 DVD42 上的信息进行加密的加密密钥的分级情况。

集成电路 41 可以在其内不存储主密钥而存储使用单向函数从主密钥计算出的诸加密密钥预定级的一加密密钥。在该情况下，当由该加密密钥或由比上述加密密钥级低的一加密密钥加密的信息是记录在 DVD42 的上面，DVD 播放机 43 能够对记录在 DVD42 上的信息进行解码。

将预定的加密密钥存储在预定的集成电路中并装在 DVD 播放机 43 内的方法适合于分配同样的加密密钥的装置而不管 DVD 的标题的情况如何。

如上所述，由于加密密钥是使用单向函数分级的，使用诸分级的加密密钥中的任意级的一个加密密钥可以对信息解码和将这个加密密钥分配给用户，用户能够通过保留最后加密密钥对先前的加密密钥加密的信息解码。这样加密密钥能被容易地管理。

图 12 示出作为例子的实施例，它能更有效地应用到加密密钥不容易通过网络交换的情况。特别是，当信息例如软件或移动图象使用预定级的一加密密钥被加密和被记录在 DVD42 上时，集成电路 41 在其中存储主密钥，这样任意级的加密密钥能通过使用单向函数(F)从主密钥中形成。这样，使用记录在 DVD42 上的预定级的加密密钥加密的信息能被解码。

因此，即使因为先前的加密密钥被解密，该加密密钥被更新，和使用新分级的加密密钥加密的信息被记录在 DVD42 上，用户使用通常的方法仍能满意地解码和再现这样的信息。

因此若没将该加密密钥存储在 DVD 播放机的集成电路 41 内则不能够正确地再现 DVD42 中记录的该加密密钥加密的信息。信息的使用能被适当地限制。进而，由于计算机不具有存储加密密钥的解码板，则不能正确地重现

记录介质其中含有由加密密钥加密的信息，信息的使用能被适当地限制。

进而，加密密钥是以复制在例如 DVD 的记录介质或复制在 DVD 的装置上的字母数字字符、条码、或全息图的形式分配的，对应于加密密钥的数据被存储在 IC 卡上，由此对应于加密密钥(例如主密钥)的数据被存储在很难被非法使用的集成电路内，对应于加密密钥的数据被插入解码软件中，或对应于加密密钥的数据通过电话网络线或网络被加以分配，这样加密密钥能被极容易地分配。

如上所述，当 DVD 用作为记录介质时，记录介质并不局限 DVD 和其它的记录介质例如 CD - ROM(密集盘只读存储器)MD(小型盘，注册商标)、光盘、磁光盘或软盘均可被使用。

本发明可应用到通过例如 Internet 的网络提供信息的情况。

当 DVD 播放机本身按如上所述在预定的存储器内存储了幻数时，本发明并不局限于此，例如，该幻数可以记录在 DVD 预定的部分，此后，它能被读出和输入到解码电路 14(图 6)。在该情况下，如图 5 所示，幻数被提供给记录装置 54 和由此记录在盘 1 上。

虽然计算机使用上述的软件解码加密的信息，下述的变化也是可能的。即，并不使用软件而依据本发明将 IC 芯片装入到计算机内而 IC 芯片可以解码加密的信息。在这种情况下，由于计算机不具有存储了加密密钥的集成电路 41，也就不能够正确解码加密的信息，信息的使用能适当地被限制。

根据本发明的加密方法和解码方法，由于诸加密密钥是使用单向函数分级的，保留最后一个加密密钥的解码侧可以解码在先加密密钥的信息。因此，当加密密钥被更新时，诸加密密钥的级(分级)能很容易地加以管理。

进而，依照本发明的加密装置和解码装置，由于加密密钥是使用单向函数从存储在第一存储器的主密钥中计算出来的和解码装置是根据存储在第二存储器中的加密密钥对信息进行解码的，持有主密钥的解码侧能够对从主密钥计算出的加密密钥加密的信息进行解码。这样，当加密密钥被更新时，诸加密密钥的级(分级)能容易地被管理。进而，由于上述的各个装置均被装置在单一的芯片内，这样就能抑制诸加密密钥的泄露，这样就可能做到高可靠地保密。

参照附图已经详细地描述了本发明的最佳实施例。应当理解，本发明并不局限那些精确的实施例，在不脱离本发明权利要求限定的本发明的构思或范围内，对本领域技术人员来说，各种变化和修改均是可能的。

图 1

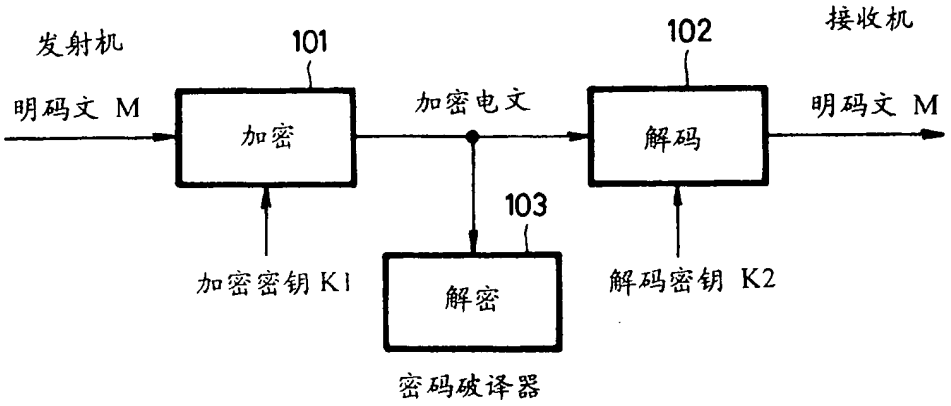
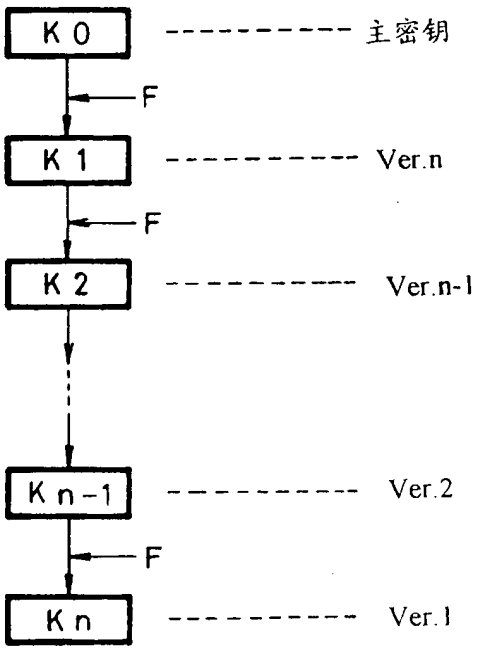

发射机
101
102
接收机
明码文 M
加密
加密电文
解码
明码文 M
103
加密密钥 K1
解密
解码密钥 K2
密码破译器

图 2


K 0
主密钥
F
K 1
Ver.n
F
K 2
Ver.n-1
K n-1
Ver.2
F
K n
Ver.1

F： 单向函数

图 3

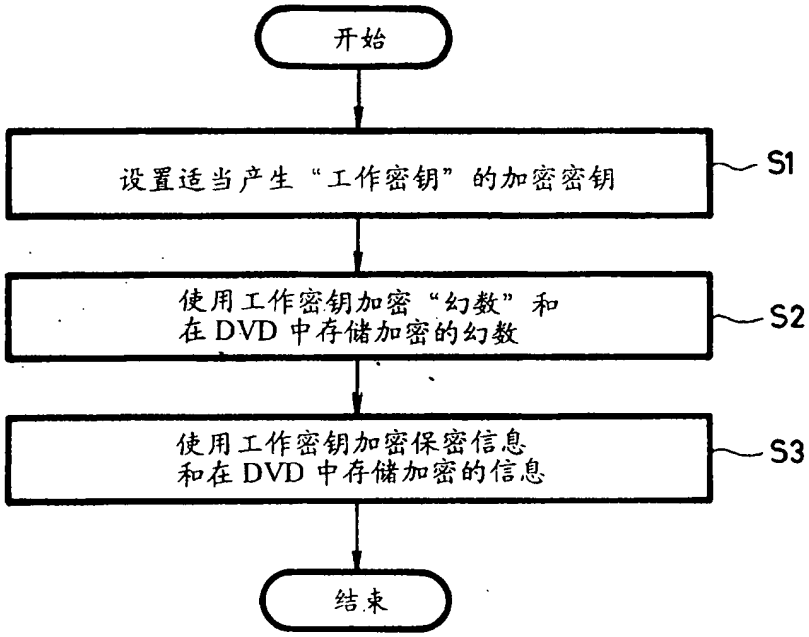

开始
设置适当产生“工作密钥”的加密密钥
S1
使用工作密钥加密“幻数”和
在 DVD 中存储加密的幻数
S2
使用工作密钥加密保密信息
和在 DVD 中存储加密的信息
S3
结束

图 4

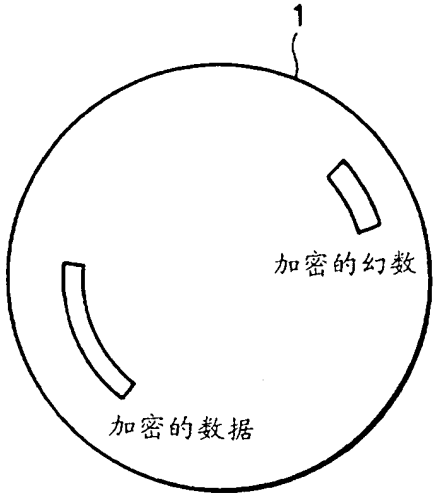

1
加密的幻数
加密的数据

图 5

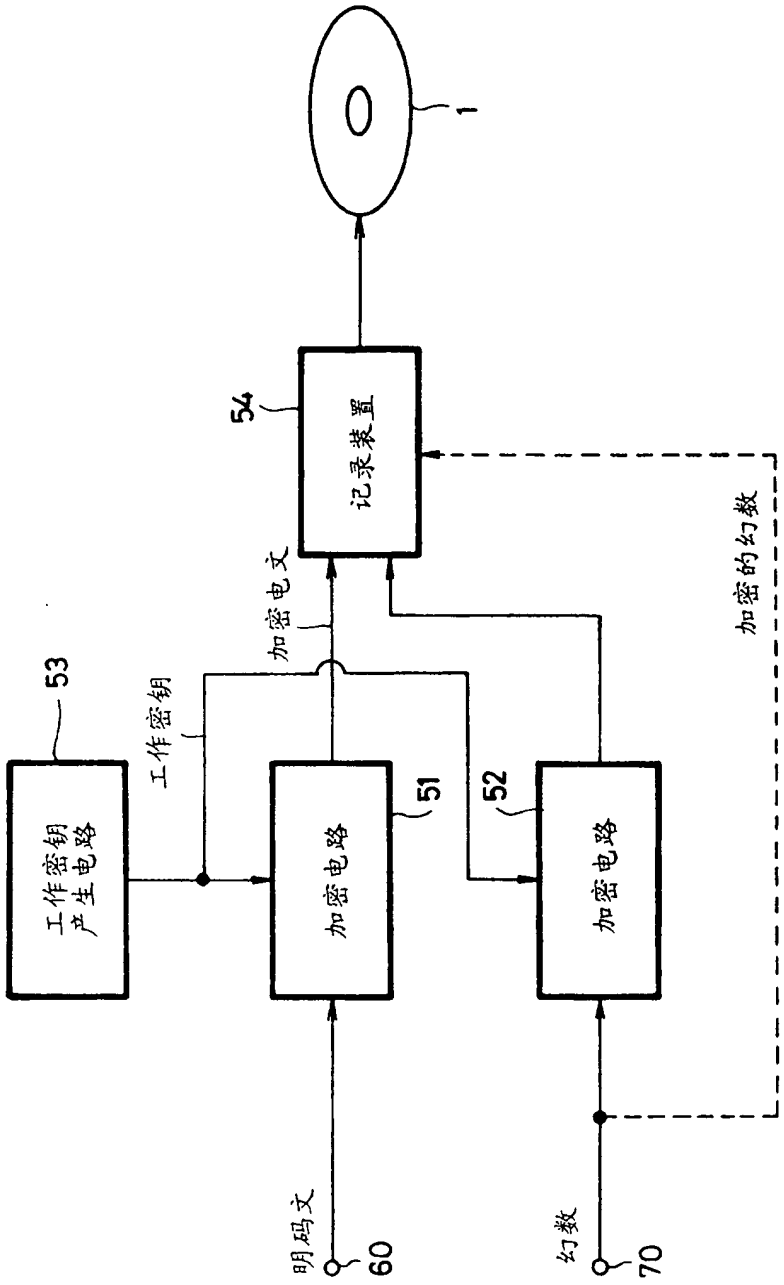

1
54
记录装置
加密的幻数
加密电文
工作密钥
53
工作密钥产生电路
加密电路
51
52
加密电路
明码文
60
幻数
70

图 6

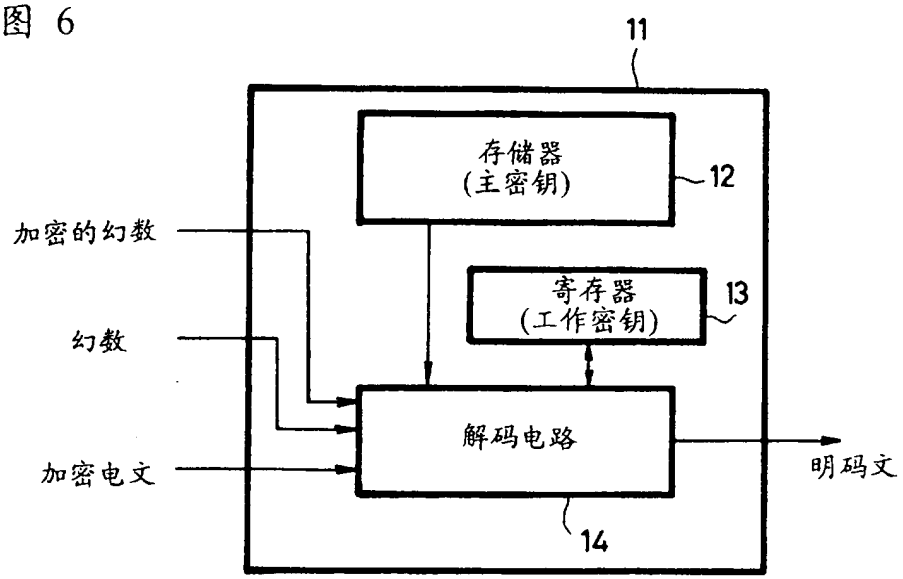

11
存储器
(主密钥)
12
加密的幻数
寄存器
(工作密钥)
13
幻数
解码电路
加密电文
明码文
14

图 7

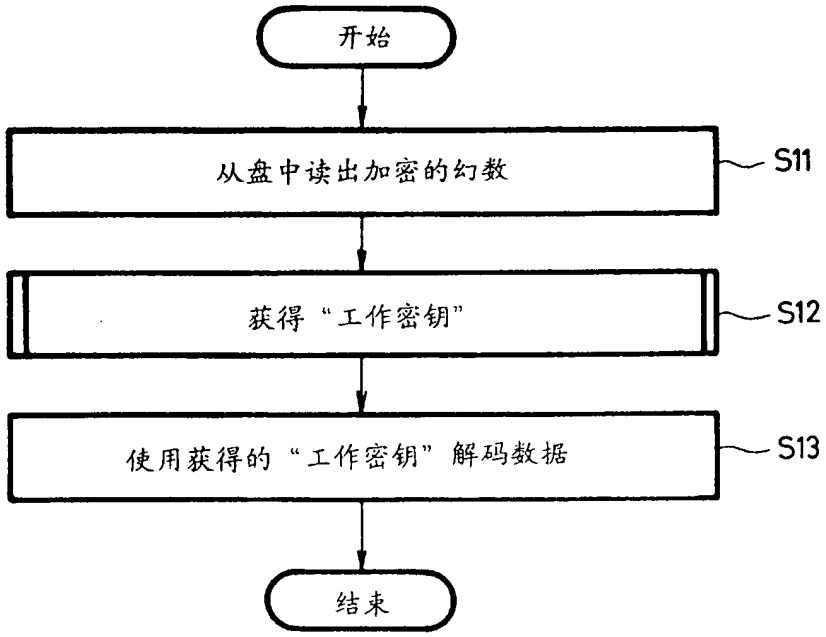

开始
从盘中读出加密的幻数
S11
获得“工作密钥”
S12
使用获得的“工作密钥”解码数据
S13
结束

图 8

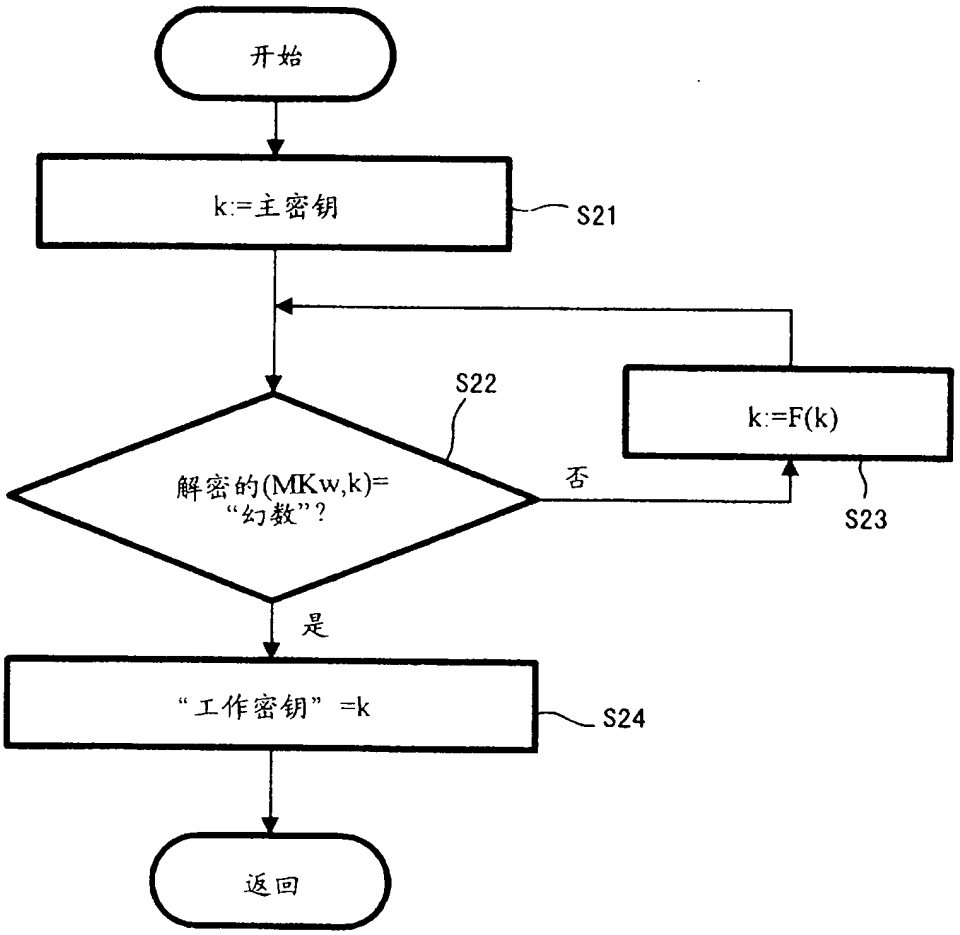


图 9

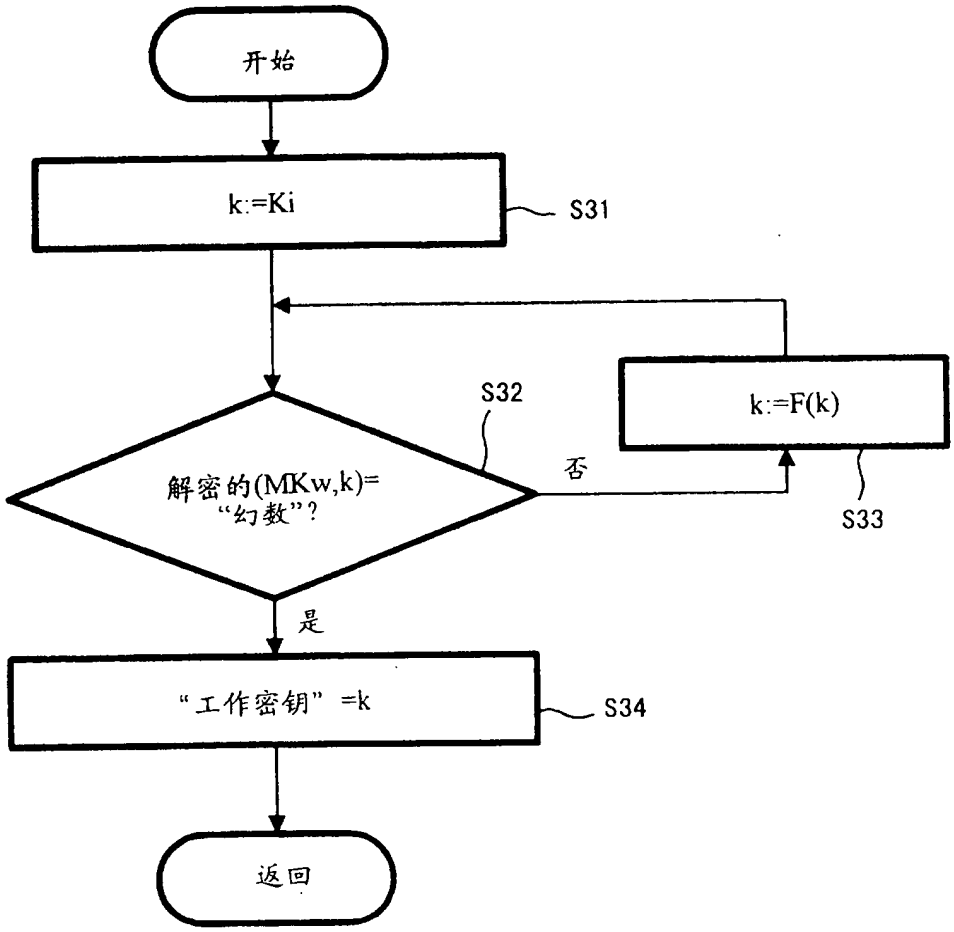


图 10

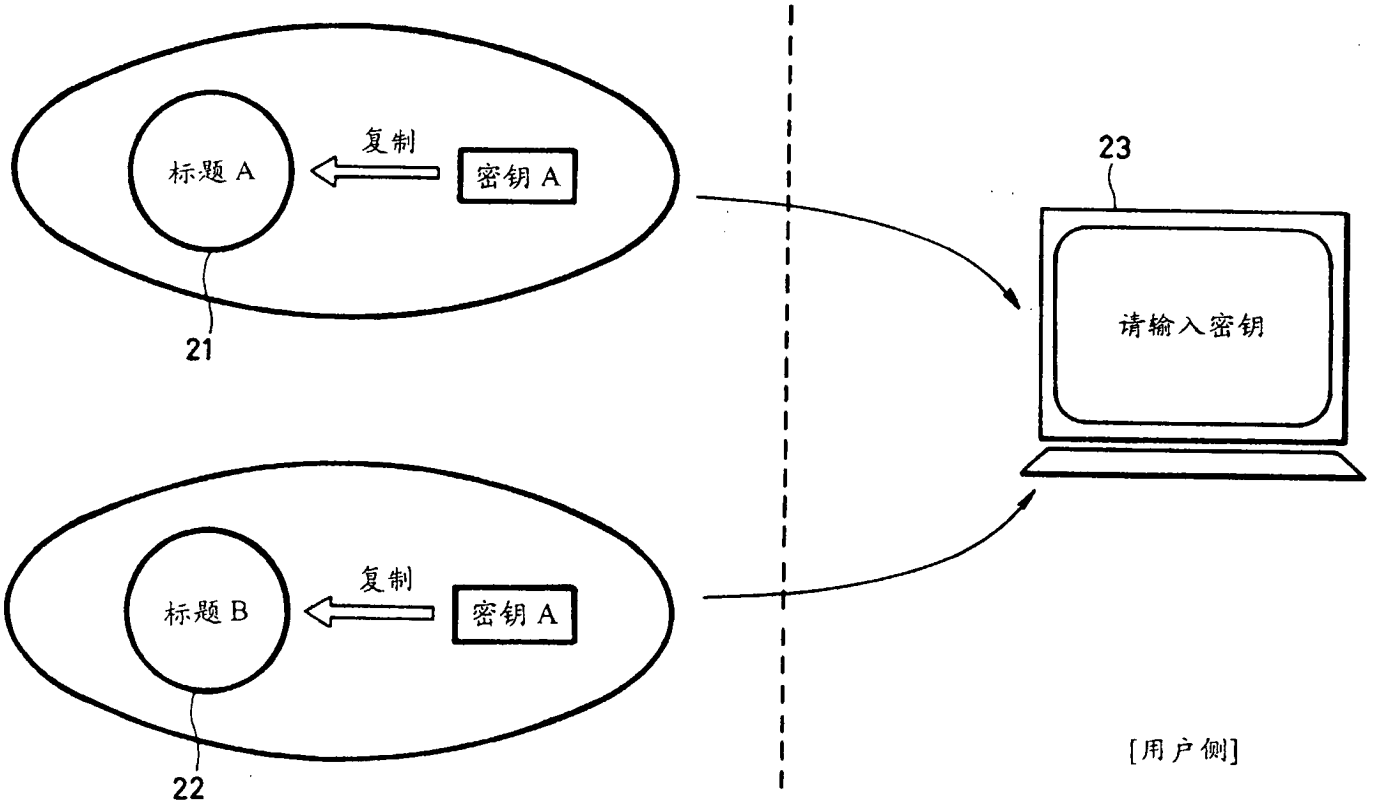


图 11

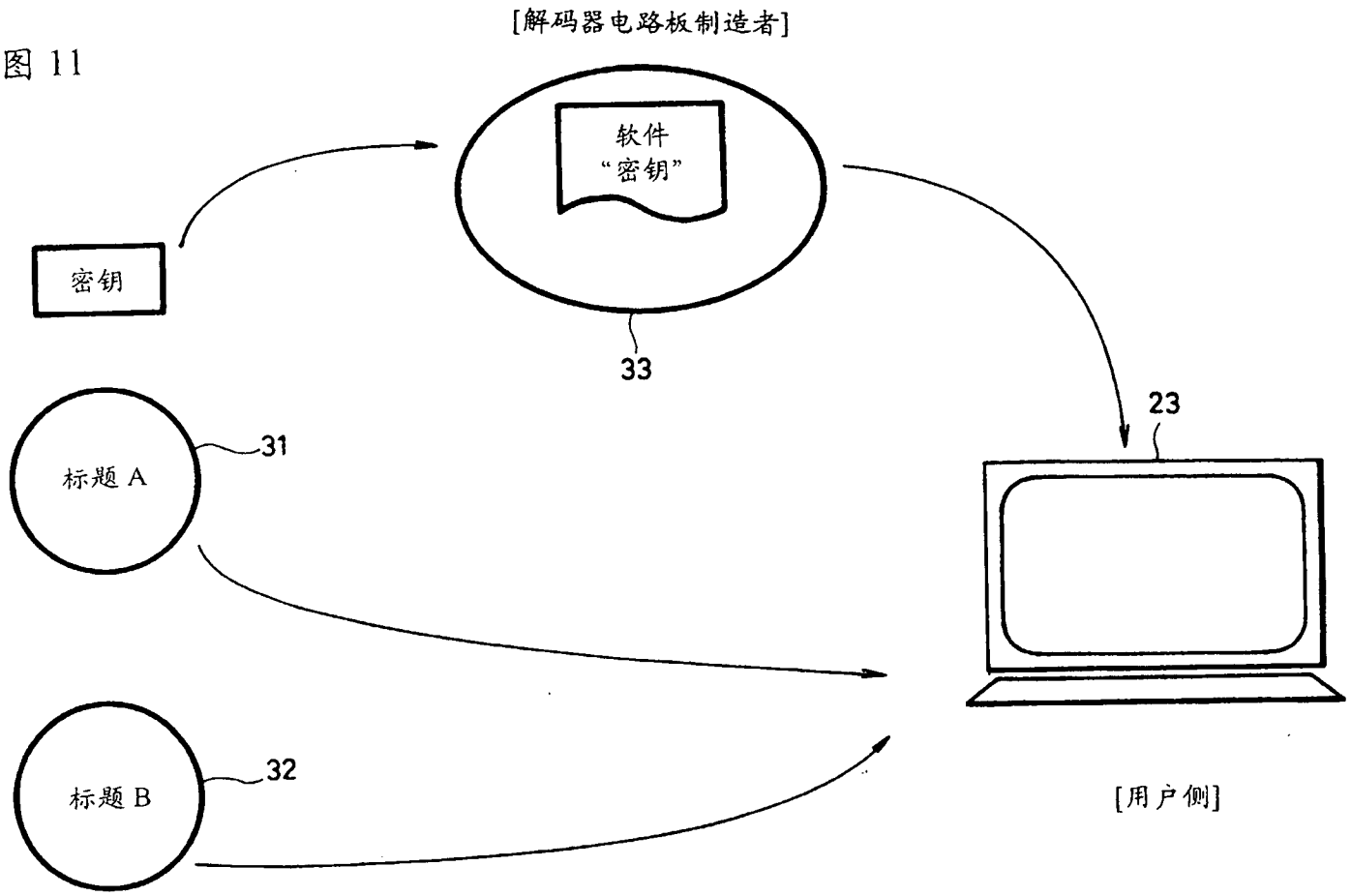
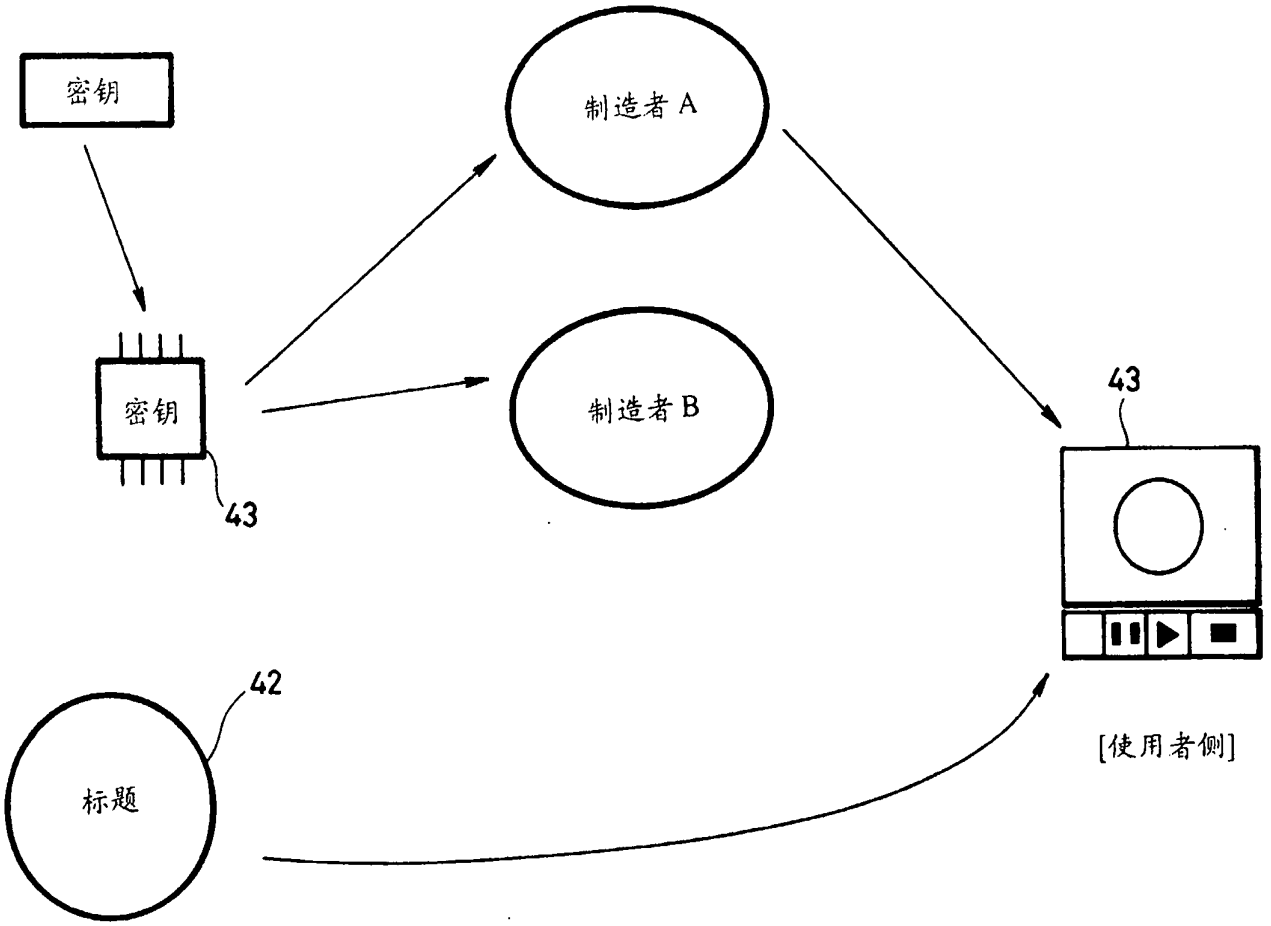


图 12



...cryption method, encryption apparatus, recording method, decoding ...ethod, decoding apparatus and recording medium

Patent number:	CN1159112
Publication date:	1997-09-10
Inventor:	ISHIGURO RYUJI (JP)
Applicant:	SONY CORP (JP)
Classification:	
- international:	H04L9/00
- european:	G11B20/00P; H04L9/08
Application number:	CN19960121033 19961016
Priority number(s):	JP19950267250 19951016

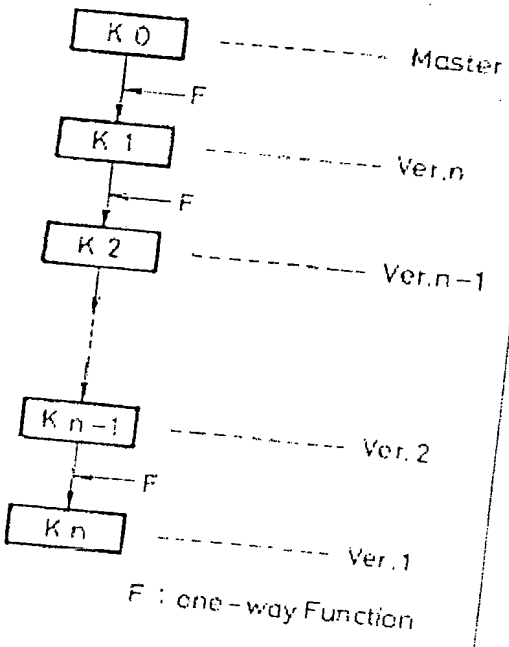
Also published as:
- EP0768774 (A2)
- US5796839 (A1)
- EP0768774 (A3)
- PL182259B (B1)
- PL182122B (B1)

Abstract not available for CN1159112

Abstract of corresponding document: **EP0768774**

In an encryption method, an encryption apparatus, a recording method, a decoding method, a decoding apparatus and a recording medium, encryption keys (K0 - Kn) can be managed with ease by hierarchizing encryption keys using a one-way function (F).

FIG. 2



Encryption method, encryption apparatus, recording method, decoding method, decoding apparatus and recording medium

Claims of corresponding document: **EP0768774**

1. A method of encrypting predetermined information by using a predetermined encryption key comprising the steps of:

hierarchizing said encryption key by using a one-way function; and
decoding said predetermined information by using said hierarchized encryption key.

2. A method as claimed in claim 1, in which a first hierarchized encryption key of said hierarchized encryption keys is a master key.

3. A method as claimed in claim 1, in which specific information is encrypted by using said hierarchized encryption key.

4. A method of recording predetermined encrypted information on a recording medium comprising the steps of:

receiving predetermined information encrypted by using an encryption key hierarchized by a one-way function; and
recording said encrypted predetermined information on said recording medium.

5.A method according to claim 4, further comprising the steps of receiving specific information encrypted by using said encryption key and recording said encrypted specific information on said recording medium together with said encrypted predetermined information.

6. A method of decoding encrypted predetermined information comprising the steps of:

receiving encrypted predetermined information; and
decoding said encrypted predetermined information by using a decoding key corresponding to an encryption key hierarchized by using a one-way function.

7. A method as claimed in claim 6, in which a first hierarchized encryption key of said hierarchized encryption keys is a master key and a decoding key corresponding to an encryption key is generated from said master key by using said one-way function.

8.A method according to claim 6, further comprising the steps of receiving encrypted specific information, determining a decoding key corresponding to an encryption key, which encrypts said received encrypted predetermined information from specific information, encrypted specific information and information used to

determine a decoding key corresponding to an encryption key, and decoding said encrypted predetermined information by using a determined decoding key.

9. A method as claimed in claim 8, in which said information for determining said decoding key corresponding to said encryption key is information of master key or information of latest encryption key.

10.A method as claimed in claim 8, in which said step for determining said decoding key corresponding to said encryption key comprises the steps of:

(a) decoding said encrypted predetermined information by using said information for determining a decoding key corresponding to an encryption key; and
comparing decoded specific information and said specific information and determining a decoding key corresponding to an encryption key based on a compared result.

11.A method as claimed in claim 10, in which if it is determined that said decoded specific information and said specific information agree with each other, then present information for determining a decoding key corresponding to an encryption key is a decoding key for decoding encrypted predetermined information, and if it is determined that said decoded specific information and said specific information do not agree with each other, then present information for determining a decoding key corresponding to an encryption key is hierarchized by using a one-way function and a decoding key corresponding to an encryption key is determined by repeating said steps (a) and (b).

12.A method as claimed in claim 6, in which said encrypted predetermined information is recorded on a recording medium, said encrypted predetermined information is read out from said recording medium and supplied, and said encryption key is printed on said recording medium or a case for storing said recording medium in the form of characters, numerals, bar code or hologram corresponding to said encryption key.

13. A method as claimed in claim 6, in which said encryption key is inserted into a predetermined software for decoding encrypted predetermined information as a code corresponding to said encryption key.

14. A method as claimed in claim 6, in which said encryption key is supplied through a telephone line network or a network.

15.An apparatus for decoding predetermined information by using a predetermined encryption key comprising:

means for generating encryption keys by hierarchizing encryption keys by using a one-way function; and
means for decoding said predetermined information by using said hierarchized encryption keys.

16. An apparatus as claimed in claim 15, in which a first hierarchized encryption

key of said hierarchized encryption keys is a master key.

17. An apparatus according to claim 15, further comprising means for encrypting specific information by using said hierarchized encryption keys.

18.An apparatus for decoding encrypted predetermined information comprising:

means for receiving said encrypted predetermined information; and
means for decoding said encrypted predetermined information by using a decoding key corresponding to encryption keys hierarchized by using a one-way function.

19. An apparatus according to claim 18, further comprising a first memory for storing information used to determine a decoding key corresponding to said encryption key, means for generating a decoding key corresponding to an encryption key from said master key by using a one-way function and a second memory for storing a decoding key corresponding to said generated encryption key and wherein information for determining a decoding key corresponding to said encryption key is a master key which is a first hierarchized encryption key of said hierarchized keys.

20.An apparatus according to claim 18, further comprising means for receiving encrypted specific information and wherein said generating means determines a decoding key corresponding to an encryption key which encrypts said received encrypted predetermined information from specific information, encrypted specific information and information for determining a decoding key corresponding to an encryption key and said decoding means decodes said encrypted predetermined information by using a determined decoding key.

21. An apparatus as claimed in claim 20, in which said information for determining a decoding key corresponding to an encryption key is information of master key or information of a latest encryption key.

22. An apparatus as claimed in claim 21, in which said generating means decodes said encrypted predetermined information by using said information for determining a decoding key corresponding to an encryption key, compares decoded specific information and said specific information and determines a decoding key corresponding to an encryption key based on a compared result.

23.An apparatus as claimed in claim 22, in which if it is determined that said decoded specific information and said specific information agree with each other, then said generating means determines that present information for determining a decoding key corresponding to an encryption key is a decoding key for decoding encrypted predetermined information and stores said decoding key in said second memory and if it is determined that said decoded specific information and said specific information do not agree with each other, then said generating means hierarchizes present information for determining a decoding key corresponding to said encryption key by using a one-way function and determines a decoding key corresponding to an encryption key by repeating operations claimed in claim 22.

24.An apparatus as claimed in claim 19, in which said first memory, said second

memory, said generating means and said decoding means are disposed within a single IC chip.

25. An apparatus as claimed in claim 24, in which said information for determining a decoding key corresponding to said encryption key is previously stored in said first memory.

26. A recording medium decodable by a decoding apparatus, in which said recording medium includes a recording signal decodable by said decoding apparatus and said recording signal contains predetermined information encrypted by encryption keys hierarchized by using a one-way function.

27. A recording medium as claimed in claim 26, in which said recording signal further includes specific information encrypted by using said encryption key.

28. A recording medium as claimed in claim 26, in which said encryption key is printed on said recording medium in the form of characters, numerals, bar code or hologram corresponding to said encryption key.

Encryption method, encryption apparatus, recording method, decoding method, decoding apparatus and recording medium

Description of corresponding document: **EP0768774**

This invention relates to encrypting information (such as software or data), recording encrypted information, decoding encrypted information, and record media in which information is recorded. A preferred form of implementation of the invention described hereinbelow provides a method of and apparatus for encrypting software or data, an apparatus for decoding encrypted software or data, a method of recording encrypted software or data, a method of decoding encrypted software or data, an apparatus for decoding encrypted software or data and a recording medium for use in preventing illegal use of software or data recorded on a recording medium such as a digital video disk or software or data supplied through a network.

In order to prevent illegal use of software or data, it is customary that software or data is encrypted by use of predetermined encryption keys and encrypted software or data is recorded on a digital video disk (hereinafter simply referred to as "DVD") or supplied through a network to thereby provide encrypted software or data. The encrypted software or data recorded on the DVD or the encrypted software or data supplied through the network is decoded by the encryption keys provided separately.

The manner in which information is encrypted and decoded will be described below in brief.

FIG. 1 of the accompanying drawings shows a principle by which information or data is encrypted and decoded.

A sender encrypts (101) plain text M (information to be transmitted) by using an encryption key K1 to provide cipher text C (data to be transmitted in actual practice). The cipher text C is transmitted to a receiver and the receiver decodes (102) the cipher text C by using a decoding key K2 to provide plain text M. In this way, plain text is transmitted from the sender to the receiver. It is frequently observed that those who have no decoding key (i.e., code-breakers) wiretap cipher text C and decodes (103) cipher text C. The manner in which those who have a decoding key generate plain text M from cipher text C is generally referred to as "decoding" while those whose have no decoding key wiretap cipher text C and get plain text M from cipher text C is referred to as "decryption".

However, when plain text is encrypted by the above-mentioned encryption key, once the encryption key is decrypted, such encryption key becomes ineffective for preventing illegal use. Therefore, when the encryption key is decrypted, the encryption key is updated to new one and software or data is encrypted by using such updated encryption key, thereby preventing illegal use of software or data.

However, in actual practice, even when the encryption key is updated, it is frequently observed that there exist encrypted software or data encrypted by the

previous encryption key. Therefore, the previous key for decoding such software or data has to be retained. As a consequence, each time the encryption key is updated, encryption keys to be retained are increased, and the hardware and the software both face problems of managing the retained encryption keys.

When the encryption key is previously assembled from a hardware standpoint, it is sometimes very difficult to update such encryption keys into new ones.

According to a first aspect of the present invention, there is provided a method of encrypting predetermined information by using a predetermined encryption key which comprises the steps of hierarchizing the encryption key by using a one-way function and decoding the predetermined information by using the hierarchized encryption key.

According to a second aspect of the present invention, there is provided a method of recording predetermined encrypted information on a recording medium which comprises the steps of receiving predetermined information encrypted by using an encryption key hierarchized by a one-way function and recording the encrypted predetermined information on the recording medium.

According to a third aspect of the present invention, there is provided a method of decoding encrypted predetermined information which comprises the steps of receiving encrypted predetermined information and decoding the encrypted predetermined information by using a decoding key corresponding to an encryption key hierarchized by using a one-way function.

According to a fourth aspect of the present invention, there is provided an apparatus for decoding predetermined information by using a predetermined encryption key which is comprised of means for generating encryption keys by hierarchizing encryption keys by using a one-way function and means for decoding the predetermined information by using the hierarchized encryption keys.

According to a fifth aspect of the present invention, there is provided an apparatus for decoding encrypted predetermined information which is comprised of means for receiving the encrypted predetermined information and means for decoding the encrypted predetermined information by using a decoding key corresponding to encryption keys hierarchized by using a one-way function.

In accordance with a sixth aspect of the present invention, there is provided a recording medium decodable by a decoding apparatus. The recording medium includes a recording signal decodable by the decoding apparatus and the recording signal contains predetermined information encrypted by encryption keys hierarchized by using a one-way function.

The preferred form of implementation of the invention described hereinbelow provides an encryption method, an encryption apparatus, a recording method, a decoding method, a decoding apparatus and a recording medium in which encryption keys can be managed with ease by hierarchizing encryption keys.

The invention will now be further described, by way of illustrative and non-limiting example, with reference to the accompanying drawings, in which:

FIG. 1 is a schematic diagram showing a principle by which software or data is encrypted and encrypted software or data is decoded;
FIG. 2 is a schematic diagram showing an example of a hierarchial structure of encryption keys which can be applied to an encryption method embodying the present invention;
FIG. 3 is a flowchart illustrative of a manner in which a DVD on which encrypted information is recorded is made;
FIG. 4 is a schematic diagram showing a DVD on which there are recorded encrypted magic key and encrypted information;
FIG. 5 is a block diagram showing an example of an encryption apparatus embodying the present invention;
FIG. 6 is a block diagram showing an example of an IC chip 11 for decoding information recorded on the DVD shown in FIG. 4;
FIG. 7 is a flowchart to which reference will be made in explaining operation of the IC chip 11 shown in FIG. 6;
FIG. 8 is a flowchart to which reference will be made in explaining the detail of a step S12 shown in FIG. 7;
FIG. 9 is a flowchart to which reference will be made in explaining the detail of the step S12 shown in FIG. 7;
FIG. 10 is a schematic diagram used to explain a manner in which encryption keys are printed on DVDs and distributed;
FIG. 11 is a schematic diagram used to explain a manner which an encryption key is inserted into decoding software and distributed; and
FIG. 12 is a schematic diagram used to explain a manner in which an encryption key is incorporated into an integrated circuit and distributed.

Embodiments of the invention will now be described with reference to the drawings.

FIG. 2 is a schematic diagram showing a manner in which encryption keys are hierarchized to which an encryption method embodying the present invention is applied.

As shown in FIG. 2, an encryption key K1 of the next hierarchy (Ver.n) is formed relative to an encryption key of the first hierarchy (master key) K0 by using a so-called one-way function) F. The one-way function F is one of so-called one-way functions and carries out an irreversible calculation in which the encryption key K1 can be easily calculated from the encryption key K0 but the reverse calculation cannot be performed substantially, i.e., the encryption key K0 cannot be substantially calculated from the encryption key K1.

On the other hand, as the one-way function, there may be used encryption algorithm such as Data Encryption Standard (DES, National Bureau of Standards FIPS Publication 46, 1977), Fast Encryption Algorithm (FEAL, S. Miyaguchi. The FEAL cipher family. Lecture Notes in Computer Science, 537 (1001), pp. 627 to 638. (Advances in Cryptology - CRYPTO '90) or a message digest algorithm such as Message Digest algorithm (MD4, R. L. Rivest. 537 (1001), pp. 303 to 311. (Advances in Cryptology - CRYPTO '90) or Secure Hash Standard (SHS, Secure Hash Standard, National Bureau of Standards FIPS Publication 180, 1993). DES

and FEAL were described in detail in "Cipher and Information Security by Tsujii and Kasahara, July 1993".

Subsequently, the one-way function will be described in detail with reference to examples.

In the case of DES, the one-way function and the DES have therebetween established a relationship expressed by the following equation (1):
"(1)" F(k) = DES(IV, k)
where IV is the Initial Vector and arbitrary and k is the key.

Moreover, as algorithm used in one-way function, there may be used the following ones:

Block cipher (product cipher)-based algorithm; and
Arithmetic algorithm

The block cipher (product cipher)-based algorithm can obtain cipher text by encrypting plain text by using a key as expressed by the following equation (2):
"(2)" C = Enc (P, k)
where C is the cipher text, p is the plain text, and k is the key.

Specifically, a bit string of fixed length is obtained by effecting irreversible transform on the key by a certain kind of hash function at every block.

Then, the plain text is processed by permutation box or substitution box for substituting data or the like several rounds. In each round, the plain text is processed by a certain calculation with the bit string obtained from the key, e.g., logical calculation of exclusive-OR.

The arithmetic algorithm is used in a problem of discrete logarithm as expressed by the following equation (3):
"(3)" F(k) <==> ak mod p
where a is the predetermined constant, k is the key and p is the prime number.

In the above equation (3), symbol "<==>" means " definition".

Specifically, function F(k) is defined as "remainder which results from dividing product multiplied with k by p". In this case, the function F(k) can be obtained from the key (k) with ease but it is very difficult to obtain the key (k) from the function F (k).

As described above, after the encryption key K1 was obtained from the master key by using the one-way function (F), encryption keys K2, K3, ..., Kn-1, Kn are sequentially calculated by using the one-way function (F) as expressed by the following equation (4), thereby resulting in hierarchized encryption keys (Ver.n through Ver.1) being formed:
"(4)" ki = F(Ki-1)
where i = 1, 2, 3, ..., n)

The numerical value n is the sufficient number of hierarchies (number of generations).

Accordingly, although new encryption keys can be calculated with ease by using the one-way function (F) as described above, the reverse calculation cannot be carried out substantially, i.e., the original key cannot be calculated substantially from the encryption keys by using the one-way function (F).

A method of encrypting information such as software or data and providing encrypted information to the user embodying the present invention will be described below. When information such as software or data is encrypted and provided to the user, as shown in FIG. 2, information is initially encrypted by using the encryption key Kn (Ver.1) and the encrypted key Kn is distributed to the user in the formed of either being attached to the encrypted information or being supplied separately. The user can decode the encrypted information by using the encryption key Kn.

When this encryption key Kn is decrypted, information such as software or data is encrypted by the encryption key Kn-1 of higher hierarchy (Ver.2) and the encryption key Kn-1 is distributed to the user. Similarly, each time an encryption key is decrypted, information is encrypted by using an encryption key of higher hierarchy and the encrypted key is distributed to the user.

The encryption key Kn of lowest hierarchy (Ver.1) initially distributed is calculated from the encryption key Kn-1 of the next hierarchy by using the function (F). Specifically, the encryption key Kn can easily be calculated by using the function (F) and information encrypted by the encryption key Kn can be decoded by using the encryption key Kn calculated from the encryption key Kn-1. Accordingly, since the encryption key is calculated from the encryption key of the next hierarchy by using the function (F), the next encryption key can be calculated by using the function (F) in any generation. Therefore, if the user retains the latest encryption key which is not decrypted, then the user can decode not only information encrypted by the latest encryption key but also information encrypted by a previous encryption key. Moreover, all encryption keys are keys that are sequentially generated from the master key by using the one-way function (F). Accordingly, if the user retains the master key instead of the latest encryption key which is not decrypted, then the user can decode information encrypted by all encryption keys. Thus, the encryption keys can be managed with ease.

FIG. 3 is a flowchart used to explain a manner in which information (plain text) such as moving image, sounds, data or software is encrypted and recorded on a recording medium such as a disk (e.g., DVD and hereinafter referred to as "DVD"), for example, by using the encryption keys shown in FIG. 2.

Referring to FIG. 3, following the start of operation, an encryption key of a proper generation (hierarchy) is selected from hierarchized encryption keys shown in FIG. 2 at a step S1 and the selected encryption key is set to a work key. Then, control goes to a step S2, wherein a string of predetermined numerals and characters is set to a magic number, the magic number is encrypted by the work key obtained at the step S1 and the encrypted magic number obtained by the encryption is recorded on a predetermined portion of a DVD 1 as shown in FIG. 4, for example.

Thereafter, control goes to a step S4, whereat encrypted data, i.e., plain text data is encrypted by using the work key and encrypted data (cipher text) is recorded on a predetermined portion of the DVD 1 as shown in FIG. 4.

An encryption apparatus corresponding to the above-mentioned encryption method will be described with reference to FIG. 5.

As shown in FIG. 5, plain text data and magic number are supplied to terminals 60 and 70, respectively. The plain text data and the magic number from the terminals 60, 70 are respectively supplied to corresponding encryption circuits 51, 52. The magic number is the string of predetermined numerals and characters as described above. A work key generating circuit 53 selects an encryption key of a proper generation (hierarchy) from the hierarchized encryption keys shown in FIG. 2 and supplies the selected encryption key to the encryption circuits 51, 52 as a work key. The encryption key 52 encrypts the supplied magic number by using the work key supplied thereto from the work key generating circuit 53. Then, encrypted magic number thus obtained by encryption is supplied to a recording apparatus 54.The encryption circuit 51 encrypts the supplied plain text data by using the work key and supplies the encrypted information to the recording apparatus 54. The recording apparatus 54 records the encrypted information and the encrypted magic information on the predetermined positions of the DVD 1 as shown in FIG. 4.

If the recording apparatus 54 is a formatter for generating a master disk, then a stamper is formed from the master disk and a large number of disks are produced by using such stamper.

FIG. 6 is a block diagram showing an IC chip for decoding encrypted information recorded on the DVD 1 in a disk player (DVD player and hereinafter referred to as "DVD player") for playing back the thus made DVD 1. Magic number, encrypted magic number and encrypted information(cipher text) are inputted to an IC chip 11. The encrypted magic number is supplied from the DVD 1, the magic number is stored in a memory (not shown) of the DVD player itself and supplied from such memory. This magic number is a string of predetermined numerals and characters. This magic number is the same as that used in the encryption side.

A memory 12 stores the encrypted key K0 shown in FIG. 2, i.e., master key. A register 13 stores an encryption key of a predetermined generation obtained by using the above function (F) relative to the master key, i.e., work key as will be described later on. A decoding circuit 14 generates a work key based on the inputted magic number, the encrypted magic number and the master key read out from the memory 12 and supplies the thus formed work key to the register 13 as will be described later on. The decoding circuit 14 decodes the inputted and encrypted information (cipher text) by using the work key and outputs the decoded data as plain text data (plain text).

The manner in which the encrypted data recorded in the DVD 1 within the IC chip 11 is decoded will be described with reference to a flowchart of FIG. 7.

Referring to FIG. 7, following the start of operation, in a step S11, the encrypted magic number is read out from the predetermined position of the DVD 1. Then,

control goes to a step S12, whereat a work key is obtained from the encrypted magic number read out at the step S1 and the magic number read out from the memory (not shown) of the DVD player itself as will be described later on with reference to a flowchart of FIG. 8.

FIG. 8 is a flowchart used to explain the processing at the step S12 in FIG. 7 more in detail.

Referring to FIG. 8, following the start of operation, initially, at a step S21, a master key is read out from the memory 12 of the IC chip 11 and set to a selection key (k). Then, this selection key (k) is supplied to the decoding circuit 14. The selection key (k) expresses an encryption key that is selected at present.

As shown in FIG. 8, control goes to the next decision step S22, whereat the magic number and the encrypted magic number are supplied to the decoding circuit 14 and thereby the encrypted magic number is decoded by using the selection key (k). Then, it is determined at the decision step S22 whether or not the result which results from decoding the encrypted magic number by the selection key (k) agrees with the magic number. If the decoded result and the magic number which is not encrypted do not agree with each other as represented by a NO at the decision step S22, then it is determined that this selection key is not the encryption key which encrypts the encrypted magic number on the encryption side.Then, control goes to a step S23, whereat an encryption key of the next generation is calculated from the selection key (k) by using the one-way function (F) as expressed by the following equation (5) and set to a new selection key (k):

"(5)" $k = F(k)$

Then, control goes back to the step S22 and the similar processing is executed repeatedly.

If on the other hand the result which results from decoding the encrypted magic number by the selection key (k) and the magic number which is not encrypted agree with each other as represented by a YES at the decision step S22, then it is determined that the selection key (k) is the encryption key which encrypts the encrypted magic number. Then, control goes to a step S24, wherein the decoding circuit 14 selects this selection key (k) as a work key and supplies this selection key (k) to the register 13, in which it is registered. Then, processing in the flowchart of FIG. 8 is ended and control goes back to the processing of the flowchart of FIG. 7.

Thereafter, control goes to a step S13 in the flowchart of FIG. 7, whereat the decoding circuit 14 reads out the work key obtained at the step S12 (steps S21 to S24 shown in FIG. 8) from the register 13, decodes the encrypted information (cipher text) inputted to the decoding circuit 14 by using the work key and outputs the decoded information as plain text data (plain text).

As described above, since the IC chip 11 obtains the work key corresponding to the encrypted information from the master key and decodes the inputted encrypted information by using this work key, if the user retains only this master key, then the user can decode information encrypted by an encryption key of any hierarchy.

When the above-mentioned processing is carried by a software of computer, the processing at the step S12 of FIG. 7 is replaced with a flowchart shown in FIG. 9. FIG. 9 is a flowchart showing a manner in which encrypted information is decoded in a computer which realizes the function shown in FIG. 6 by software. In this case, the computer incorporates therein a decoding board corresponding to FIG. 6 and software is memorized in a memory of such decoding board. Moreover, in this case, a master key that is previously stored in the memory is not used but a latest encryption key (or may be a master key) to be distributed is used.

As will be described later on with reference to FIG. 10, for example, the user inputs an encryption key (Ki) (where i represents any one of n, n-1, ..., 1) of a predetermined hierarchy distributed in the form of being printed on the DVD through a keyboard to a computer. Such encryption key is memorized in a predetermined memory disposed within the computer. Alternatively, the computer receives the latest encryption key distributed through a telephone network line or a network and stores a predetermined memory (e.g., RAM (random-access memory)).

Referring to FIG. 9, following the start of operation, at a first step S31, inputted encryption key (Ki) of a predetermined hierarchy is read out from the memory and set to a selection key (k). The selection key (k) expresses an encryption key selected at present similarly as described above.

Then, control goes to a decision step S32, whereat a magic number read out from the memory and an encrypted magic number read out from the DVD are supplied and the encrypted magic number is decoded by the selection key (k). In the decision step S32, it is determined whether or not a result which results from decoding the encrypted magic number by the selection key (k) and the magic number agree with each other. If the decoded result and the magic number which is not encrypted do not agree with each other as represented by a NO at the decision step S32, then it is determined that the selection key (k) is not the encryption key which encrypts the encrypted magic number.Therefore, control goes to a step S33, whereat an encryption key of the next generation is calculated from the selection key (k) by using a one-way function (F) and the thus calculated encryption key of the next generation is set to a new selection key (k).

Then, control goes back to the step S32 and the similar processing is repeatedly executed.

If on the other hand the result which results from decoding the encrypted magic number by the selection key and the magic number agree with each other as represented by a YES at the decision step S32, then it is determined that the selection key (k) is the encryption key which encrypts the encrypted magic number. Therefore, control goes to the next step S34, whereat this selection key (k) is set to the work key and this work key is stored in a predetermined memory (e.g., register). Then, the processing in the flowchart of FIG. 9 is ended and control goes back to the flowchart of FIG. 7.

Thereafter, control goes to the step S13 of the flowchart shown in FIG. 7, whereat encrypted information is decoded by using the work key obtained at the step S12 (steps S31 to S34 shown in FIG. 9) and outputted as plain text data (plain text).

As described above, when information encrypted by the software of the computer is decoded, it is possible to decode information encrypted by at least the encryption key (Ki) or encryption keys (Ki-1 through K1) of hierarchies lower than the encryption key (Ki) based on the encryption key of arbitrary hierarchy distributed.

As described above, according to the embodiment of the present invention, since information encrypted by the previous encryption keys can be decoded based on the latest encryption key (may be master key or encryption key of arbitrary hierarchy), it is sufficient that only the latest encryption key is memorized. Therefore, unlike the prior art, in addition to the previous encryption keys, new encryption keys need not be memorized and managed each time an encryption key is decrypted and an encryption key is varied. Thus, encryption keys can be managed with ease.

Further, in the embodiment shown in FIG. 6, since the encryption key (master key) is stored in the memory 12 disposed within the IC chip 11, an encryption key of a predetermined hierarchy is calculated within the IC chip 11 and encrypted information is decoded, the encryption key can be prevented from being leaked to the outside and decryption of the encryption key can be made difficult. Further in the above-mentioned embodiment, since the processing for calculating the work key and the processing for decoding the encrypted information can be carried out by the same decoding circuit 14, the circuit can be saved.

The manner in which encryption keys are distributed will be described with reference to FIGS. 10 to 12.

FIG. 10 illustrates the manner in which encryption keys are printed on a case of DVD or DVD itself and distributed.

As shown in FIG. 10, alphanumeric character, bar code, hologram or the like corresponding to an encryption key of a predetermined hierarchy is printed on a case of a DVD 21 with a title A recorded thereon or the surface of the DVD 21 itself. Similarly, alphanumeric character, bar code, hologram or the like corresponding to an encryption key B of a predetermined hierarchy is printed on a case of a DVD 22 with a title B recorded thereon or the surface of the DVD 22 itself. In this manner, the encryption key A can be distributed to the user together with the DVD 21 and the encryption key B can be distributed to the user together with the DVD 22.
Alternatively, data indicative of the encryption key A may be recorded on a recording medium such as an IC card and distributed to the user together with the DVD 21 or data indicative of the encryption key B may be recorded on a recording medium such as an IC card and distributed to the user together with the DVD 22.

When the user plays back the DVD 21, the user enters the encryption key A printed on the DVD 21 into a computer 23 by using an input apparatus such as a keyboard. As described above with reference to the flowchart shown in FIG. 9, the computer 23 executes the function that the IC chip 11 shown in FIG. 6 executes, i.e., the function for decoding encrypted information in accordance with a predetermined application program.

Then, when the DVD 21 is set on a DVD reader (not shown), the computer 23

reads out the encrypted information from the DVD 21 through the DVD reader and decodes the encrypted information read out from the DVD 21 based on the previously-entered encryption key A. Of course, encrypted information recorded on the DVD 22 can be decoded in the same way as in the DVD 21.

Accordingly, this case is suitable for distributing different encryption keys at every title of DVD. For example, encryption keys computed from different master keys by one-way function may be assigned to every title of DVD.

Furthermore, even when the encryption key A corresponding to the title A is decrypted, the encryption key A corresponding to the title A is updated to an encryption key A2 of higher hierarchy and continuation information of the title A is encrypted by the encryption key A2, the encryption key A that is not yet updated can be easily obtained from the encryption key A2 by a predetermined computation similarly as described above with reference to the flowchart of FIG. 9. Therefore, the user can decode the title A encrypted by the previous encryption key by using only the latest encryption key (in this case, the encryption key A2).

FIG. 11 illustrates the manner in which a code indicative of encryption key is inserted into software for decoding an encryption key and distributed to the user.

As shown in FIG. 11, a code indicative of encryption key is inserted into decoding software provided on a decoding board 33 for decoding encryption information. Then, this decoding board 33 is loaded onto the computer 23. Thus, the computer 23 can decode encrypted information recorded on DVDs 31, 32 through the decoding board 33 and output moving picture, still picture and sounds corresponding to decoded information.

This example is suitable for distributing the same encryption key to the user.

In the case of this example, the computer 23 may be connected to a telephone network line or a network, whereby updated encryption key may be distributed to the computer 23 through the telephone network line or the network. The computer 23 memorizes the latest encryption key distributed thereto through the telephone network line or the network in the software for decoding the decoding board 33.

Then, the computer 23 can decode information recorded on the DVDs 31, 32 by using this encryption key similarly as described above with reference to FIGS. 7 and 9.

Further, information encrypted by the encryption key can be supplied to the computer 23 through the telephone network line or the network. In this case, the computer 23 decodes this information by using the encryption key previously distributed through the telephone network line or the network.

As described above with reference to FIG. 2, encryption keys of all hierarchies can be formed from the hierarchized first encryption key (K0) by using the one-way function (F) and this encryption key K0 can be used as the master key. Therefore, if the encryption key serving as the master key is inserted into a hardware such as an integrated circuit (IC), then encryption keys of all hierarchies can be formed from this encryption key K0 and even information encrypted by any one of encryption

anduandbandd

keys (K1 through Kn) can be decoded. Since it is very difficult for the users to decrypt data inserted into the hardware such as the integrated circuit, illegal use of the encryption key can be suppressed.

FIG. 12 illustrates the manner in which an encryption key is inserted into an integrated circuit and distributed. As shown in FIG. 12, a maker having a legal obligation to keep secret manufactures an integrated circuit 41 in which a master key is stored. The IC chip 11 can be applied to the integrated circuit 41. In the case of this example, the integrated circuit 41 is supplied to a maker A. Then, after the integrated circuit 41 was assembled into a DVD player 43, the integrated circuit 41 is distributed to the user.

On the other hand, magic number encrypted by using an encryption key of a predetermined hierarchy memorized in the integrated circuit 41 and predetermined encryption information encrypted by this encryption key are recorded on a DVD 42.

When the user sets the DVD 42 on the DVD player 43, a master key is read out from the integrated circuit 41 and a work key is obtained in the same manner as that described with reference to the flowcharts shown in FIGS. 7 and 8, whereby encrypted information recorded on the DVD 42 is decoded and corresponding moving picture, still picture and sounds can be outputted.

When the master key is memorized in the integrated circuit as described above, the DVD player 43 is able to decode and output encrypted information recorded on the DVD 42 regardless of hierarchy of encryption key which encrypts the information recorded on the DVD 42.

The integrated circuit 41 may memorize therein not the master key but an encryption key of a predetermined hierarchy of encryption keys computed from the master key by using a one-way function. In that case, when information encrypted by that encryption key or an encryption key of hierarchy lower than that of the above encryption key is recorded on the DVD 42, the DVD player 43 can decode the information recorded on the DVD 42.

The method in which a predetermined encryption key is memorized in a predetermined integrated circuit and assembled into the DVD player 43 is suitable for the case wherein the same encryption key is distributed regardless of the title of DVD.

As described above, since the encryption key is hierarchized by using the one-way function, information is decoded by using an encryption key of arbitrary hierarchy of the hierarchized encryption keys and this encryption key is distributed to the user, the user can decode information encrypted by the previous encryption key only by retaining the latest encryption key. Thus, encryption keys can be managed with ease.

The embodiment shown in FIG. 12, for example, can be more effectively applied to the case wherein encryption keys cannot be interchanged easily through a network. Specifically, when information such as software or moving picture is encrypted by an encryption key of a predetermined hierarchy and recorded on the DVD 42, the

anduandbandd

integrated circuit 41 memorizes the master key therein so that an encryption key of an arbitrary hierarchy can be formed from this master key by using the one-way function (F). Thus, the information encrypted by the encryption key of the predetermined hierarchy recorded on the DVD 42 can be decoded.

Therefore, even if the encryption key is updated and information encrypted by an encryption key of a new hierarchy is recorded on the DVD 42 because the previous encryption key is decrypted, the user can decode and reproduce such information satisfactorily in a usual manner.

Since DVD players which do not have the integrated circuit 41 with encryption keys stored therein are unable to correctly reproduce the DVD 42 in which information encrypted by this encryption key is recorded, use of information can be limited properly. Further, since computers which do not have the decoding board in which encryption keys are memorized are unable to correctly reproduce a recording medium in which information encrypted by the encryption key, use of information can be limited properly.

Furthermore, encryption keys are distributed in the form of alphanumeric characters, bar code or hologram printed on the recording medium such as DVD or the case of DVD, data corresponding to the encryption key is memorized in the IC card, data corresponding to an encryption key (e.g., master key) is memorized in the integrated circuit which is difficult to be used illegally, data corresponding to the encryption key is inserted into the decoding software or data corresponding to the encryption key is distributed through the telephone network line or the network, whereby the encryption key can be distributed extremely easily.

While the DVD is used as the recording medium as described above, the recording medium is not limited to the DVD and other recording media such as CD-ROM (compact disc-read-only memory), MD (minidisc, registered trademark), optical disk, magnetooptical disk or floppy disk can be used.

The present invention can be applied to the case that information is provided through a network such as Internet.

While the DVD player itself stores the magic number in a predetermined memory as described above, the present invention is not limited thereto and the magic number may be recorded on a predetermined portion of DVD, for example, whereafter it may be read out and inputted to the decoding circuit 14 (FIG. 6). In that case, as shown in FIG. 5, the magic number is supplied to the recording apparatus 54 and thereby recorded on the disk 1.

Although the computer decodes encrypted information by using software as described above, the following variant is also possible. That is, software is not used and an IC chip embodying the present invention may be incorporated within the computer and the IC chip may decode encrypted information. In this case, since computers which do not have the integrated circuit 41 in which encryption keys are memorized are unable to correctly decode encrypted information, use of information can be limited properly.

According to the encryption method and the decoding method described above,

since encryption keys are hierarchized by using the one-way function, the decoding side which retains the latest encryption key can decode information encrypted by the previous encryption key. Therefore, the generation (hierarchy) of encryption keys can be managed with ease when the encryption key is updated.

Further, according to the encryption apparatus and the decoding apparatus described above, since encryption keys are calculated from the master key memorized in the first memory by using the one-way function and the decoding means decodes information based on the encryption key memorized in the second memory, the decoding side which holds the master key can decode information encrypted by the encryption key computed from the master key. Therefore, the generation (hierarchy) of encryption keys can be managed with ease when the encryption key is updated. Furthermore, since the above-mentioned respective means are disposed within the single chip, the leakage of encryption keys to the outside can be suppressed, thereby making it possible to make security highly reliable.

Having described preferred embodiments of the invention with reference to the accompanying drawings, it is to be understood that the invention is not limited to those precise embodiments and that various changes and modifications could be effected therein by one skilled in the art without departing from the scope of the invention as defined in the appended claims.